

STATEMENT OF THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
October 16, 2003

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to discuss Internet vulnerabilities and the dangers they pose to citizens, businesses and governments. My testimony today will focus on the Federal government's response to this growing cyber threat.

Dangers and Vulnerabilities presented by the Internet

The Internet connects over 171,000,000 computers and continues to expand at a rapid pace. At any point in time, there are millions of connected computers that are vulnerable to worms, viruses or denial of service attacks. Malicious actors can take advantage of these vulnerable machines and harness them together to create large scale attacks. Many attacks are fully automated and spread with blinding speed across the entire Internet community.

The private sector has become increasingly dependent on the Internet and now uses it for mission critical applications as well as online business transactions. Even relatively short interruptions in service can cause significant economic loss and can jeopardize critical services.

Similarly, the Federal government's reliance on the Internet will continue to grow in the years ahead. The healthy functioning of cyberspace will be essential to our homeland and national security.

Awareness of Internet Dangers

The Federal Computer Incident Response Center (FedCIRC) within the Department of Homeland Security is the Federal government's focal point for coordinating response to cyber attacks (non-law enforcement), promoting incident reporting, and cross-agency sharing of data about common vulnerabilities. As part of its duties, FedCIRC informs Federal agencies about current and potential security threats from the Internet.

Working with FedCIRC, OMB and the CIO Council have developed a process to rapidly counteract identified threats and vulnerabilities. CIOs are advised via conference call, as well as follow up e-mail, of specific actions needed to protect agency systems. Agencies must then report through FedCIRC to OMB on the implementation of the required countermeasures. In

particular, we track data concerning the percentage of systems patched and the time needed to complete mitigation efforts.

FedCIRC maintains a strong relationship with a number of industry as well as government partners. These partners include commercial software vendors, Carnegie Mellon University's Computer Emergency Response Team, law enforcement, the intelligence community, and agency incident response teams. These organizations routinely communicate advance notice to DHS regarding the discovery of software vulnerabilities and the development of malicious code designed to exploit these weaknesses.

Steps the Federal Government is Taking to Protect Itself from this Growing Threat

National Institute of Standards and Technology

Securing cyberspace is an ongoing process, as new technologies appear and new vulnerabilities are identified. The National Institute of Standards and Technology (NIST) provides timely guidance to federal agencies on securing networks, systems, and applications. NIST recommends that agencies implement a patch management program, harden all hosts appropriately, deploy antivirus software to detect and block malicious code, and configure the network perimeter to deny all traffic that is not necessary. Additional recommendations include user awareness briefings as well as training for technical staff on security standards, procedures, and sound security practices. Per longstanding OMB policy, Federal agencies are directed to follow NIST guidelines.

NIST has produced a number of recent publications that address agency security practices. These publications include: a Guide to IT Security Services, Selecting Information Security Products, Network Security Testing, Building an IT Security Awareness and Training Program, and Security Considerations in the Information Systems Development Life Cycle. Earlier guidance included: Securing the Public Web Server, Electronic Mail Security, IT Contingency Planning, Security Metrics, System Administrator Guidance for Securing Win 2000, Wireless Security, Security Patch Management, Intrusion Detection Systems, Firewall Security, and Risk Management.

As part of its statutory responsibilities under the Federal Information Security Management Act, the National Institute of Standards and Technology published in September a draft Computer Security Incident Handling Guide. This publication seeks to help both established and newly formed incident response teams respond effectively and efficiently to a variety of incidents. More specifically, this document discusses organizing a computer security incident response capability, establishing incident response policies and procedures, structuring an incident response team, and handling incidents from initial preparation through the post-incident lessons learned phase. Finally, it discusses handling a range of incidents, such as denial of service, malicious code, unauthorized access, inappropriate usage, and multiple component incidents.

Federal Information Security Management Act

Another critical mechanism used to enforce protection of Federal systems is the Federal Information Security Management Act (FISMA). Under FISMA, Federal agencies are required to periodically test and evaluate the effectiveness of their information security policies, procedures and practices. The results of both the agency self assessments and the IG assessments are provided to OMB each September. OMB submits a summary report to Congress based on the agency and IG reports.

Federal Enterprise Architecture

Improving the federal government's response to Internet based attacks also requires that we focus on enterprise architecture and the standardized deployment of security technologies. As new technologies become available and cost effective, they must be incorporated into the IT infrastructure where they can monitor common precursors and indications of attack.

Challenges Facing the Federal Government in Creating a More Secure Cyber-Environment

Attack Attribution

Because of the global nature of cyberspace, vulnerabilities are accessible to anyone anywhere with sufficient capability to exploit them. Discerning the source of malicious activity is often difficult. The federal government will continue to rely on federal, state and local law enforcement to investigate and prosecute developers of worms, viruses and denial of service attacks. Agencies must continue to report computer incidents and assist law enforcement investigations to the greatest extent possible.

Managing Vulnerabilities inherent in Commercial Software

Vulnerabilities result from weaknesses in technology as well as improper implementation and oversight of technological products. The National Strategy to Secure Cyberspace recommends that the software industry consider promoting more secure "out of the box": installation and implementation of their products, including increasing user awareness and user friendliness of their security features.

Use of Security Benchmarks

OMB supports agency use of enterprise licensing agreements which require vendors to configure software to meet security benchmarks. As an example, the Department of Energy recently signed an agreement with Oracle Corporation which calls for the vendor to deliver its database software in a securely configured manner.

Use of Trusted Products

In addition, the federal government will soon begin a comprehensive review of the National Information Assurance Partnership (NIAP). One thing they will consider is to what extent, if any, NIAP can address the continuing problem of security flaws in commercial software products. This review will include lessons-learned from implementation of the Defense

Department's July 2002 policy requiring the acquisition of products reviewed under the NIAP evaluation process.

Patch Management

Because of software vulnerabilities, patch management is an essential part of an agency's information security program and requires a substantial investment of time, effort and resources. Agencies must carefully follow predefined processes in order to successfully remediate system vulnerabilities across the enterprise.

These processes include: identifying all affected systems and related software revision levels, fully testing the patch before it is placed into a production environment, and prioritizing installation of the patch based on the criticality of the system. Alternative solutions such as judicious use of port blocking must be implemented if the patch cannot be installed.

At the present time, forty-seven agencies subscribe to FedCIRC's Patch Authentication and Dissemination Capability. This service validates and quickly distributes corrective patches for known vulnerabilities.

Conclusion

The Federal government is the world's largest consumer of information technology. Because of its vast inventory and the vulnerabilities inherent in commercial software, the Federal government will, for the immediate future, continue to be impacted by threats from the Internet. Through our oversight of agency security policies and practices, OMB will continue to work with agencies to ensure that the risks associated with cyber attacks are appropriately mitigated.

In closing, OMB is committed to a federal government with resilient information systems. The dangers posed by the Internet must not be allowed to significantly affect agency business processes or disrupt services to the citizen. OMB will continue to work with agencies and the Congress to ensure that appropriate countermeasures are in place to reduce the impact of Internet borne attacks.